Claims:

1. A system for executing application software on a operating system within a secured run-time environment without affecting an application software resources of a client computer, the system comprising:

an application wrapper, wherein said application wrapper shields the application software resources, whereby said secured run-time environment for executing said application software is created and the application software resources are protected; and

the application wrapper further comprising a privatized virtual file resource created from an operating system file system, a privatized virtual registry created from an operating system registry system, a privatized operating system shared component resource, a privatized application configuration resource and a privatized environmental resources for application variables.

2. The system of claim 1, wherein privatized virtual file resource further comprising:

intercepting file I/O request generated by one or more processes;

establishing a process ID for the intercepted file I/O request;

comparing process ID to establish operating system process and secured run-time process;

establishing a process ID as operating system process and secured run-time process;

servicing the file I/O request for all process ID established as secured run-time process;

redirecting the file I/O request to operating system service for process ID established as operating system process;

rejecting the file I/O request on secured run-time process resources for process ID established as operating system process;

comparing process ID established as secured run-time process to further establish process resources corresponding to process ID;

establishing corresponding process resources within secured run-time resources; and

rejecting the file I/O request on secured run-time process resources for process ID established as secured run-time process and process ID belongs to other process resources.

3. The system of claim 1, wherein privatized virtual registry further comprises:

privatizing virtual registry system by intercepting registry I/O request generated by several process;

establishing process ID for the intercepted registry I/O request;

comparing process ID to establish operating system process and secured run-time process;

establishing process ID as operating system process and secured run-time process;

servicing the registry I/O request for all process ID established as secured run-time process;

redirecting the registry I/O request to operating system service for process ID established as operating system process;

rejecting the registry I/O request on secured run-time process resources for process ID established as operating system process;

comparing process ID established as secured run-time process to further establish process resources corresponding to process ID;

establishing corresponding process resources within secured run-time resources; and

rejecting the registry I/O request on secured run-time process resources for process ID established as secured run-time process and process ID belongs to other process resources.

4. The system of claim 1, wherein privatizing operating system shared component resource further comprising:

searching secured application process for injecting component hooker;

checking the said secured application process to establish whether the process is injected with component hooker;

establishing the said secured application process as new secured application process for said secured application process not injected with component hooker;

injecting component hooker to new secured application process to intercept component process;

repeating component hooker injection for all the new secured application process;

5. The system of claim 1, wherein privatizing operating system shared component resource further comprising:

Initializing component redirection table to provide component redirecting information;

Registering virtual component required for the secured application;

Adding redirecting information to the said component redirection table for the execution of each selected said secured run-time application;

Removing component redirecting information from the said component redirection table for the termination of each said secured run-time application;

6. The system of claim 1, wherein privatizing operating system shared component resource further comprising:

intercepting component process function for replacing component search path with secured application resource path;

replacing component search path with private resource path to load the component from the secured application resource path; and

creating new process for the intercepted component with the replaced secured application resource path.

7. The system of claim 1, wherein privatizing operating system shared component resource further comprising:

intercepting component call for replacing component registry path with the said privatized virtual registry path;

searching component redirection table for the said component redirecting information;

replacing component registry path with the said privatized virtual registry path retrieved from the said component redirection table;

returning the intercepted call to the requested call with the replaced secured application registry path for addressing the component location from the privatized virtual registry system and further the said component is addressed to load from the said privatized virtual file system;

redirecting the said component call as it is to the requested call for the said component call originated from non secured run-time application and for the said component call, which do not have redirecting information in the said component redirection table.

8. The system of claim 1, wherein privatizing operating system shared component resource further comprising:

intercepting the said RPC message call for replacing component information with privatized virtual component information;

searching component redirecting information from the said component redirection table;

replacing RPC message with the said privatized virtual component information retrieved from the said component redirection table;

returning the intercepted RPC message call to the requested call with the replaced message;

continuing the RPC call to locate the privatized virtual component through SCM;

redirecting the said RPC message call as it is to the requested call for the said component call originated from non secured run-time application and for the said component call, which do not have redirecting information in the said component redirection table.

9. The system of claim 1, wherein privatized application configuration resource further comprises:

monitoring file I/O request for configuration file to provide separate configuration file;

searching and retrieving configuration file from secured application resources; and

serving application configuration file to requesting process.

10. The system of claim 1, wherein privatized environmental resources further comprises:

intercepting environment variable request to supply private values to secured application process;

verifying process ID to establish the process ID as operating system process or secured application process;

redirecting the call for process ID established as operating system process;

reading variable data from secured application resource and returning the value to requested process for read variable calls requested by the secured application process;

searching the requesting write variable in secured application resource to find the presence of requesting write variable;

creating variable with variable data within secured application resource and returning the status to requested process for variable do not exist in secured application resource; and updating variable with variable data within secured application resource and returning the status to requested process for variable exist in secured application resource.

11. The system of claim 1, wherein the application wrapper further comprises selectively allowing the application software to interact operating system resources directly during the said application software executing under the said secured run-time environment.

12. The system of claim 1, wherein the application wrapper further comprises selectively allowing said application software to interact with other application software resources directly during the said application software executing under the said secured run-time environment.

13. The system of claim 1, wherein said application wrapper further comprises providing a run-time environment to said application software that is visible to an operating system run-time environment without having said application software run-time resources, whereby said application software resources is simulated to said secured run-time environment during the execution of said application software.

14. The system of claim 13, further comprising means for protecting the behavior of said application software from other application and said operating system.

15. The system of claim 13, further comprising means for eliminating said application conflicts from other running application software.

16. The system of claim 13, further comprising means for executing multiple instance of single said application software.

17. The system of claim 1, wherein the said application wrapper further comprising maintaining the application software resources away from said operating system resources, whereby said operating system resources is protected from said application software resources.

18. The system of claim 1, wherein said application wrapper further comprises permitting full access to said application software that requires to access for variation occurs to said application software resources within the said application wrapper.

19. The system of claim 18 further comprising means for keeping the state of secured run-time environment to said application software.

20. The system of claim 18, further comprising means for updating said application software resources required by said application software.

21. The system of claim 1, wherein the said application wrapper monitors the said application run-time request to determine the required said application software resources for execution.

22. The system of claim 21, further comprising means for receiving said application software resources to execute said application software in the said secured run-time environment.

23. The system of claim 21, further comprising means for incrementally executing the said application software in the secured run-time environment.

24. A method for executing application software on a operating system within a secured run-time environment without affecting an application software resources of a client computer, the client compute comprising an application wrapper, wherein said application wrapper shields the said application software resources, whereby a said secured run-time

environment for executing an said application software is created and the said application software resources is protected, the method further comprising:

privatizing virtual file resource created from an operating system file system;

privatizing virtual registry created from an operating system registry system;

privatizing operating system shared component resource;

privatizing application configuration resource; and

privatizing environmental resources for application variables.

25. The method of claim 24, wherein privatizing the virtual file resource further comprising:

intercepting file I/O request generated by several processes;

establishing process ID for the intercepted file I/O request;

comparing process ID to establish operating system process and secured run-time process;

establishing process ID as operating system process and secured run-time process;

servicing the file I/O request for all process ID established as secured run-time process;

redirecting the file I/O request to operating system service for process ID established as operating system process;

rejecting the file I/O request on secured run-time process resources for process ID established as operating system process;

comparing process ID established as secured run-time process to further establish process resources corresponding to process ID;

establishing corresponding process resources within secured run-time resources; and

rejecting the file I/O request on secured run-time process resources for process ID established as secured run-time process and process ID belongs to other process resources.

26. The method of claim 24, wherein Privatizing the virtual registry further comprising:

privatizing virtual registry system by intercepting registry I/O request generated by several process;

establishing process ID for the intercepted registry I/O request;

comparing process ID to establish operating system process and secured run-time process;

establishing process ID as operating system process and secured run-time process;

servicing the registry I/O request for all process ID established as secured run-time process;

redirecting the registry I/O request to operating system service for process ID established as operating system process;

rejecting the registry I/O request on secured run-time process resources for process ID established as operating system process;

comparing process ID established as secured run-time process to further establish process resources corresponding to process ID;

establishing corresponding process resources within secured run-time resources; and

rejecting the registry I/O request on secured run-time process resources for process ID established as secured run-time process and process ID belongs to other process resources.

27. The method of claim 24, wherein privatizing operating system shared component resource further comprising:

intercepting component process function for replacing component search path with secured application resource path;

replacing component search path with private resource path to load the component from the secured application resource path; and

creating new process for the intercepted component with the replaced secured application resource path.

28. The method of claim 24, wherein privatizing operating system shared component resource further comprising:

searching secured application process for injecting component hooker;

checking the said secured application process to establish whether the process is injected with component hooker;

establishing the said secured application process as new secured application process for said secured application process not injected with component hooker;

injecting component hooker to new secured application process to intercept component process;

repeating component hooker injection for all the new secured application process;

29. The method of claim 24, wherein privatizing operating system shared component resource further comprising:

Initializing component redirection table to provide component redirecting information;

Registering virtual component required for the secured application;

Adding redirecting information to the said component redirection table for the execution of each selected said secured run-time application;

Removing component redirecting information from the said component redirection table for the termination of each said secured run-time application;

30. The method of claim 24, wherein privatizing operating system shared component resource further comprising:

intercepting component call for replacing component registry path with the said privatized virtual registry path;

searching component redirection table for the said component redirecting information;

replacing component registry path with the said privatized virtual registry path retrieved from the said component redirection table;

returning the intercepted call to the requested call with the replaced secured application registry path for addressing the component location from the privatized virtual registry system and further the said component is addressed to load from the said privatized virtual file system;

redirecting the said component call as it is to the requested call for the said component call originated from non secured run-time application and for the said component call, which do not have redirecting information in the said component redirection table.

31. The method of claim 24, wherein privatizing operating system shared component resource further comprising:

intercepting the said RPC message call for replacing component information with privatized virtual component information;

searching component redirecting information from the said component redirection table;

replacing RPC message with the said privatized virtual component information retrieved from the said component redirection table;

returning the intercepted RPC message call to the requested call with the replaced message;

continuing the RPC call to locate the privatized virtual component through SCM;

redirecting the said RPC message call as it is to the requested call for the said component call originated from non secured run-time application and for the said component call, which do not have redirecting information in the said component redirection table.

32. The method of claim 24, wherein privatizing application configuration resource further comprising:

monitoring file I/O request for configuration file to provide separate configuration file;

searching and retrieving configuration file from secured application resources; and

serving application configuration file to requesting process.

33. The method of claim 24, wherein privatizing environmental resources for application variables further comprising:

intercepting environment variable request to supply private values to secured application process;

verifying process ID to establish the process ID as operating system process or secured application process;

redirecting the call for process ID established as operating system process;

reading variable data from secured application resource and returning the value to requested process for read variable calls requested by the secured application process;

searching the requesting write variable in secured application resource to find the presence of requesting write variable;

creating variable with variable data within secured application resource and returning the status to requested process for variable do not exist in secured application resource; and

updating variable with variable data within secured application resource and returning the status to requested process for variable exist in secured application resource.

34. The method of claim 24, wherein selectively allows said application software to interact operating system resources directly during the said application software executing under the said secured run-time environment.

35. The method of claim 24, wherein selectively allows said application software to interact with other application software resources directly during the said application software executing under the said secured run-time environment.

36. The method of claim 24, wherein said application wrapper provides an run-time environment to said application software that visible to be an operating system run-time environment without having said application software run-time resources, whereby said application software resources is simulated to said secured run-time environment during the execution of said application software.

37. The method of claim 36, further comprising protecting the behavior of said application software from other application and said operating system.

38. The method of claim 36, further comprising eliminating said application conflicts from other running application software.

39. The method of claim 36, further comprising executing multiple instance of single said application software.

40. The method of claim 24, wherein the said application wrapper keeps the application software resources away from said operating system resources, whereby said operating system resources is protected from said application software resources.

41. The method of claim 24, wherein said application wrapper allows full access to said application software that requires to access for variation occurs to said application software resources within the said application wrapper.

42. The method of claim 41, further comprising a means for keeping the state of secured run-time environment to said application software.

43. The method of claim 41, further comprising a means for updating said application software resources required by said application software.

44. The method of claim 24, wherein the said application wrapper monitors the said application run-time request to determine the required said application software resources for execution.

45. The method of claim 44, further comprising a means for receiving said application software resources to execute said application software in the said secured run-time environment.

46. The method of claim 44, further comprising a means for incrementally executing the said application software in the secured run-time environment.